

# ABELIAN QUOTIENTS AND ORBIT SIZES OF FINITE GROUPS

THOMAS MICHAEL KELLER AND YONG YANG

ABSTRACT. Let  $G$  be a finite group, and let  $V$  be a completely reducible faithful  $G$ -module. It has been known for a long time that if  $G$  is abelian, then  $G$  has a regular orbit on  $V$ . In this paper we show that  $G$  has an orbit of size at least  $|G/G'|$  on  $V$ . This generalizes earlier work of the authors, where the same bound was proved under the additional hypothesis that  $G$  is solvable. For completely reducible modules it also strengthens the 1989 result  $|G/G'| < |V|$  by Aschbacher and Guralnick.

## 1. INTRODUCTION

This paper is a sequel to [5]. In that paper we proved that if  $G$  is a finite solvable group and  $V$  is a completely reducible faithful  $G$ -module (possibly of mixed characteristic), then  $G$  has an orbit of size at least  $|G/G'|$  on  $V$ . In the case that  $G' = 1$ , i.e.,  $G$  is abelian, this had been known for a long time, and so the result seemed to be a natural and intuitive generalization of that fact which should, in fact, hold true for arbitrary groups. The proof, however, even just for solvable groups, turned out to be quite difficult, and in [5] we had to leave the problem for arbitrary finite groups as a conjecture.

In this paper we are able to prove this conjecture, that is, our main result is the following.

**Theorem 1.1.** *Let  $G$  be a finite group and  $V$  a finite faithful completely reducible  $G$ -module, possibly of mixed characteristic. Let  $M$  be the largest orbit size in the action of  $G$  on  $V$ . Then*

$$|G/G'| \leq M.$$

The reader should compare this result to a 1989 result of Aschbacher and Guralnick [1]. They proved that if  $V$  is a faithful  $G$ -module of characteristic  $p$  for a finite group  $G$  satisfying  $O_p(G) = 1$ , then  $|G/G'| < |V|$ . So for completely reducible  $V$  Theorem 1.1 strengthens this bound.

Interestingly, the proof of Theorem 1.1 rests on all the earlier results proved on this: We use the result for solvable groups from [5] as well as a slight generalization of the Aschbacher-Guralnick result which is presented in Lemma 2.1. In addition, and not surprisingly, the proof uses the Classification of Finite Simple Groups (CFSG).

Roughly speaking, the main idea of the proof is to bound  $|G/G'|$  by  $|T/T'|$  for a suitable nilpotent subgroup  $T$  of  $G$  and then to use the result for solvable groups. A major ingredient here is a result on finite simple groups which guarantees the existence of abelian subgroups of order larger than the order of the abelian quotient of the outer automorphism group of the group (see Section 4). The proof of this result goes through CFSG and is admittedly quite

tedious, but its usefulness makes up for that. The proof in Section 4 also uses a refinement of a result by Feit [2] on large Zsigmondy prime divisors (see Section 3).

## 2. ABELIAN QUOTIENTS AND THE FITTING SUBGROUP

We need the following generalization of a result by Aschbacher and Guralnick [1, Theorem 3].

**Lemma 2.1.** *Let  $G$  be a finite group and  $V$  a finite, faithful  $G$ -module, possibly of mixed characteristic. Suppose that  $V = F^*(GV)$ . Then*

$$|G : G'| < |V|.$$

*Proof.* Let  $G$  and  $V$  be a counterexample such that  $|GV|$  is minimal. Now assume that  $G$  acts trivially on some Sylow  $p$ -subgroup  $X$  of  $V$  for some prime  $p$ . Then  $V = X \times Y$  for a Hall  $p'$ -subgroup  $Y$  of  $V$ , and  $G$  acts faithfully on  $Y$  such that

$$Y = F^*(GY),$$

so by induction we conclude that

$$|G : G'| < |Y| \leq |V|$$

and are done. Thus we may assume that  $G$  acts nontrivially on every Sylow subgroup of  $V$  (for every prime dividing  $|V|$ ). Let  $p$  be a prime dividing  $|V|$ .

Now define

$$0 = V_0 < V_1 < \dots < V_n = V$$

for some  $n \in \mathbb{N}$  and  $G_i$  ( $i = 1, \dots, n$ ) as follows:

Let  $G_0 = G$ . Now suppose that  $G_i, V_i$  are already defined for some  $i \geq 0$ . We treat different cases separately.

Case 1:  $p$  divides  $|V/V_i|$ .

Then let  $V_{i+1}$  be such that  $V_i < V_{i+1} \leq V$  and  $W_{i+1} = V_{i+1}/V_i$  is an irreducible  $G$ -module over  $\text{GF}(p)$ . Let  $G_{i+1} = C_{G_i}(W_{i+1}) \leq G_i$ . Observe that  $G_{i+1} = C_G(W_1 \oplus \dots \oplus W_{i+1}) \leq G$ .

Case 2:  $p$  does not divide  $|V/V_i|$ .

Then we put  $m = i$ , and  $P := V_m \in \text{Syl}_p(V)$ , and we put

$$H = G_i = C_G(W_1 \oplus \dots \oplus W_m) \leq G.$$

Case 2a:  $V_m = V$ .

Then  $n = m$ , and  $V$  is a  $p$ -group. By [3, Corollary 5.3.3]  $H$  is a  $p$ -group, so  $HV$  is a nilpotent normal subgroup of  $GV$ . Hence by our hypothesis we have

$$HV \leq F^*(GV) = V,$$

so  $H = 1$ .

Case 2b:  $V_m < V$ .

Then let  $q$  be a prime dividing  $|V/V_m|$ ; clearly  $q \neq p$ . We already have  $V_m$  and  $G_m$ . Now define

$$V_m < V_{m+1} < \dots < V_t \leq V \text{ (for some } t \in \mathbb{N} \text{) and}$$

$$G_m \geq G_{m+1} \geq \dots \geq G_t \text{ recursively as follows:}$$

Suppose that  $G_j, V_j$  are already defined for some  $j \geq m$ . We again consider two subcases.

Case 2b(i):  $q$  divides  $|V/V_j|$ .

Then let  $V_j < V_{j+1} \leq V$  be such that  $W_{j+1} = V_{j+1}/V_j$  is an irreducible  $G$ -module over  $\text{GF}(q)$ . Let  $G_{j+1} = C_{G_j}(W_{j+1}) \leq G_j$ , then  $G_{j+1} \trianglelefteq G$ .

Case 2b(ii):  $q$  does not divide  $|V/V_j|$ .

Then we put  $s = j$ , and  $Q := V_i$  is a Hall  $\{p, q\}$ -subgroup of  $V$ , and we put  $L = G_j = C_G(W_1 \oplus \dots \oplus W_s) \trianglelefteq G$ . If  $V_s = V$ , then we put  $n = s$ , and  $V$  is a  $\{p, q\}$ -group. Otherwise, we continue to define the remaining  $V_i$  similarly as before, using up the remaining primes of  $|V|$  one after another. That is, if we have already defined  $V_k, G_k$  for some  $k \geq s$ , then if  $V_k = V$ , we let  $n = k$  and are done, and if  $V_k < V$ , we let  $V_k < V_{k+1} \leq V$  such that  $W_{k+1} = V_{k+1}/V_k$  is an irreducible  $G$ -module over  $\text{GF}(r)$ , where  $r$  is the prime used at that moment, and define

$$G_{k+1} = C_{G_k}(W_{k+1}).$$

In this fashion, if we write  $V = P_1 \oplus \dots \oplus P_l$  for some  $l \in \mathbb{N}$ , where  $P_i \in \text{Syl}_{p_i}(V)$  for the distinct primes  $p_i$  dividing  $|V|$ , where  $p = p_1$  and (if  $l > 1$ )  $q = p_2$ , we obtain  $t_i \in \mathbb{N}$  ( $i = 1, \dots, l$ ) such that

$$V_{t_{i+1}}/V_{t_i} \cong W_{t_{i+1}} \oplus \dots \oplus W_{t_{i+1}} \cong P_i$$

(where " $\cong$ " just stands for isomorphism as groups, not as  $G$ -modules) for  $i = 1, \dots, l$ . (Note that  $t_1 = m$  and  $t_l = n$ .)

Next we claim that for  $G_n = C_G(W_1 \oplus \dots \oplus W_n)$  we have

$$(*) \quad G_n = 1.$$

If  $V$  is a  $p$ -group, we already saw this above, so we may assume that  $V$  is not a  $p$ -group (i.e.,

$q$  exists). Now observe that  $\bigcap_{i=1}^l C_G(P_i) = 1$ , and so

$$G_n \lesssim \bigwedge_{i=1}^l G_n / C_{G_n}(P_i),$$

and by [3, Corollary 5.3.3] we know that  $G_n / C_{G_n}(P_i)$  is a  $p_i$ -group. Thus  $G_n$  is nilpotent of order having only prime divisors from  $V$ . Moreover, if  $x \in G_n$  is of  $p_i$ -power order for some  $i \in \{1, \dots, l\}$ , then  $x$  acts trivially on  $P_j$  for all  $j \neq i$ , because  $xC_{G_n}(P_j) \in G_n / C_{G_n}(P_j)$  and the latter is a  $p_j$ -group. This shows that  $G_n V$  is nilpotent, and as  $G_n V \trianglelefteq GV$ , by our hypothesis we conclude that

$$G_n V \leq F^*(GV) = V,$$

so  $G_n = 1$  follows and  $(*)$  is proved.

Next we fix  $i \in \{0, \dots, n-1\}$  and consider the action of  $H_i := G_i/G_{i+1}$  on  $W_{i+1}$ . Let  $r$  be the characteristic of  $W_{i+1}$ . Since  $W_{i+1}$  is an irreducible faithful  $G/C_G(W_{i+1})$ -module, we have that

$$O_r(G/C_G(W_{i+1})) = 1,$$

and as

$$H_i = G_i/C_{G_i}(W_{i+1}) = G_i/(C_G(W_{i+1}) \cap G_i) \cong G_i C_G(W_{i+1})/C_G(W_{i+1}) \leq G/C_G(W_{i+1}),$$

we see that also  $O_r(H_i) = 1$ .

Hence by [1, Theorem 3] (or induction) we conclude that  $|H_i : H'_i| < |W_{i+1}|$ .

Now by [5, Lemma 2.1] and since  $G_n = 1$  we have that

$$|G : G'| \leq \prod_{i=0}^{n-1} |H_i : H'_i| < \prod_{i=0}^{n-1} |W_{i+1}| = |V|.$$

This concludes the proof of the lemma. □

**Theorem 2.2.** *Let  $G$  be a finite group with  $F^*(G) = F(G)$ . Then*

$$|G : G'| \leq |F(G) : F(G)'|.$$

*Proof.* We let  $G$  be a counterexample of minimal order. Clearly  $G > 1$ . Put  $N = \Phi(F(G))$ . By [4, Lemma 3.16(a)] we have

$$(1) \quad F^*(G/N) = F^*(G)/N = F(G)/N = F(G/N).$$

So if  $N > 1$ , we may apply the induction hypothesis which yields that

$$|G : G'N| = |(G/N) : (G/N)'| \leq |F(G/N) : F(G/N)'| = |F(G)/N : (F(G)/N)'|,$$

where the last equality follows from (1). Now as  $F(G)/N$  is abelian, it follows that

$$(2) \quad |G : G'N| \leq |F(G)/N|$$

Next observe that  $F(G)' \leq N \cap G'$ . Hence we have

$$(3) \quad \frac{|N|}{|F(G)'|} \geq \frac{|N|}{|N \cap G'|} = |N : N \cap G'| = |NG' : G'|.$$

So putting (2) and (3) together gives

$$|G : G'| = |G : G'N| |G'N : G'| \leq |F(G)/N| \cdot \frac{|N|}{|F(G)'|} = |F(G) : F(G)'|,$$

so that we are done.

Hence from now on we may assume that  $N = 1$ .

Also,  $F(G)$  is abelian of squarefree exponent, and  $C_G(F(G)) = F(G)$ , so  $G/F(G)$  acts faithfully on  $F(G)$ . We have to show that  $|G : G'| \leq |F(G)|$ .

Now observe that  $F(G') = F(G) \cap G'$ . Let  $F(G) \leq K \leq G$  be such that  $K/F(G)$  is the kernel of the action of  $G/F(G)$  on  $F(G')$ . Our next goal is to show that  $K = F(G)$ .

Write

$$V_0 = V = F(G) \quad \text{and} \quad V_1 = F(G')$$

(reading  $V$  as a  $G/F(G)$ -module of possibly mixed characteristic).

Note that  $H := G/F(G)$  acts trivially on  $V/V_1$ , because if  $g \in G$  and  $x \in F(G)$ , then  $x^g = x[x, g]$  where  $[x, g] \in F(G) \cap G' = F(G')$ , so that

$$(xF(G'))^g = xF(G').$$

So  $H$  acts faithfully on  $V$  and acts trivially on both  $V/V_1$  and  $V_1$ . Let  $\Pi$  be the set of common prime divisors of  $|V/V_1|$  and  $|V_1|$ . If  $\Pi = \emptyset$ , then it is clear that  $K = F(G)$ .

So let  $\Pi \neq \emptyset$ . If  $p \in \Pi$  and  $P \in \text{Syl}_p(V)$ , then either  $K \leq C_G(P)$  or  $K/C_K(P)$  is a  $p$ -group by [3, Corollary 5.3.3]. Now let  $V = X \oplus Y$ , where  $X$  is the Hall  $\Pi$ -subgroup of  $V$ , and  $Y$  is the Hall  $\Pi'$ -subgroup of  $V$ . Clearly  $K$  acts trivially on  $Y$ , so as  $K/F(G)$  acts faithfully on  $V$ , we see that  $K/F(G)$  acts faithfully on  $X$ . Let  $p_i$  ( $i = 1, \dots, n$  for some  $n \in \mathbb{N}$ ) be the distinct prime numbers in  $\Pi$ , so that

$$X = P_1 \times \dots \times P_l$$

for  $P_i \in \text{Syl}_{p_i} X$  for  $i = 1, \dots, l$ . Write  $\bar{K} = K/F(G)$ . Then

$$\bar{K} \lesssim \bigtimes_{i=1}^l \bar{K}/C_{\bar{K}}(P_i),$$

and from the above we know that  $\bar{K}/C_{\bar{K}}(P_i)$  is a  $p_i$ -group for all  $i$ . This shows that  $\bar{K}$  is nilpotent of order divisible only by primes out of  $\Pi$ . Moreover, any  $p_i$ -element of  $\bar{K}$  can only act nontrivially on  $P_i$  and must act trivially on  $P_j$  for all  $j \neq i$ , as  $\bar{K}/C_{\bar{K}}(P_j)$  is a  $p_j$ -group. This shows that  $\bar{K}F(G)$  is nilpotent. So if  $\bar{K} > 1$ , then we may assume that  $\bar{Q}_1 \in \text{Syl}_{p_1}(\bar{K})$  is nontrivial, and then  $\bar{Q}_1 \trianglelefteq G/F(G)$ , and if  $Q_1 \leq G$  is the inverse image of  $\bar{Q}_1$  in  $G$ , then we easily see that  $F(G) < Q_1$ , and  $Q_1$  is a nilpotent normal subgroup of  $G$  (since  $\bar{Q}_1$  and thus also the Sylow  $p_1$ -subgroup of  $Q_1$  centralizes the Hall  $p'_1$ -subgroup of  $F(G)$ ), contradicting the definition of  $F(G)$ .

Thus  $\bar{K} = 1$ , and hence  $K = F(G)$ , as desired. So as  $K = F(G)$ , we now know that  $G/F(G)$  acts faithfully on  $F(G')$ , and  $F(G')$  can be viewed as a faithful  $G/F(G)$ -module of possibly mixed characteristic. Moreover, if we look at the semidirect product  $H$  of  $G/F(G)$  and  $F(G')$  with respect to the mutual action, then

$$F(G') = F^*(H),$$

because clearly  $F^*(H) = F(H)$ , and if we had  $F(H) > F(G')$ , the  $F(H)/F(G') \cong G/F(G)$  would contain a normal  $p$ -subgroup  $\bar{S} > 1$  for some prime  $p$  such that  $\bar{S}$  would act trivially on the Hall  $p'$ -subgroup of  $F(G')$  and also - since  $G$  acts trivially on  $F(G)/F(G')$  - on the Hall  $p'$ -subgroup of  $F(G)/F(G')$ . Hence (again by [3, Corollary 5.3.3])  $\bar{S}$  would act trivially on the Hall  $p'$ -subgroup of  $F(G)$ , and thus if  $S \leq G$  with  $F(G) \leq S$  is the inverse image of  $\bar{S}$  in  $G$ , then  $S \trianglelefteq G$  would be nilpotent, contradicting  $F(G) < S$ .

So indeed  $F(G') = F^*(H)$ , and hence we may apply Lemma 2.1 to the action of  $H$  on  $F(G')$ . This yields

$$|G : G'F(G)| = |H : H'| \leq |F(G')|.$$

Thus altogether

$$\begin{aligned}
|G : G'| &= |G : G'F(G)| |G'F(G) : G'| \\
&\leq |F(G')| \cdot |F(G) : (F(G) \cap G')| \\
&= |F(G')| \cdot |F(G) : F(G')| \\
&= |F(G)|,
\end{aligned}$$

which completes the proof of the theorem.  $\square$

**Corollary 2.3.** *Let  $G$  be a finite group and  $C = C_G(E(G))$ . Then*

$$|C : C'| \leq |F(G) : F(G')|.$$

*Proof.* First note that  $F^*(C) = F(C) = F(G)$ , as is well-known (see e.g. [4, Lemma 3.13(i)]). Therefore by 2.2 we conclude that

$$|C : C'| \leq |F(C) : F(C')| = |F(G) : F(G')|$$

and we are done.  $\square$

**Corollary 2.4.** *Let  $G$  be a finite group and  $C = C_G(E(G)/Z)$ . Then*

$$|C : C'| \leq |F(G) : F(G')|.$$

*Proof.* First note that  $F^*(C) = F(C) = F(G)$ , as is well-known (see e.g. [4, Lemma 3.13(i)]). Therefore by 2.2 we conclude that

$$|C : C'| \leq |F(C) : F(C')| = |F(G) : F(G')|$$

and we are done.  $\square$

### 3. NUMBER THEORY

Let  $a$  and  $m$  be integers greater than 1. A Zsigmondy prime for  $(a, m)$  is a prime  $l$  such that  $l \mid a^m - 1$  but  $l \nmid a^i - 1$  for  $1 \leq i \leq m - 1$ . A well-known theorem of Zsigmondy asserts that Zsigmondy prime exist except if  $(a, m) = (2, 6)$  or  $m = 2$  and  $a = 2^k - 1$ .

Observe that if  $l$  is a Zsigmondy prime for  $(a, m)$ , then  $a$  has order  $m$  modulo  $l$  and so  $l \equiv 1 \pmod{m}$ . Thus  $l \geq m + 1$ . A prime  $l$  is a large Zsigmondy prime for  $(a, m)$  if  $l$  is a Zsigmondy prime for  $(a, m)$  and either  $l \geq 2m + 1$  or  $l^2 \mid a^m - 1$ .

Walter Feit [2] proved the following result.

**Theorem 3.1.** *If  $a$  and  $m$  are integers greater than 1, then there exists a large Zsigmondy prime for  $(a, m)$  except in the following cases.*

- $m = 2$  and  $a = 2^s 3^t - 1$  for some natural number  $s$ , and  $t = 0$  or  $1$ .
- $a = 2$  and  $m = 4, 6, 10, 12, 18$ .
- $a = 3$  and  $m = 4$  or  $6$ .
- $a = 5$  and  $m = 6$ .

We need the following variation of Feit's result.

**Theorem 3.2.** *If  $a$  and  $m$  are integers greater than 1, then there exists a Zsigmondy prime for  $(a, m)$  such that either  $l \geq 3m + 1$  or  $l^2 \mid a^m - 1$  except in the following cases.*

- $m = 2$  and  $a = 2^s 3^t - 1$  for some natural number  $s$ , and  $t = 0$  or  $1$ .
- $a = 2$  and  $m = 3, 4, 6, 8, 10, 12, 18, 20$ .

- $a = 3$  and  $m = 4$  or  $6$ .
- $a = 4$  and  $m = 3, 6$ .
- $a = 5$  and  $m = 6$ .

*Proof.* This could be proved by following the same argument as in [2] with adjustments along the way. The calculation is subtle and tedious. Since the main ideas are the same, I do not write everything into detail.  $\square$

**Corollary 3.3.** *If  $q$  is a prime power and  $m$  is an integer greater than 1, then there exists a Zsigmondy prime  $l \mid q^m - 1$  such that either  $l \geq 2m + 1$  or  $l^2 \mid q^m - 1$  except in the following cases.*

- $m = 2$ .
- $q = 2$  and  $m = 4, 6, 10, 12, 18$ .
- $q = 3$  and  $m = 4, 6$ .
- $q = 5$  and  $m = 6$ .

*Proof.* This follows immediately from Theorem 3.1.  $\square$

**Corollary 3.4.** *If  $q$  is a prime power and  $m$  is an integer greater than 1, then there exists a prime  $l \mid q^m - 1$  such that either  $l \geq 2m + 1$  or  $l^2 \mid q^m - 1$  and  $l^2 \geq 2m + 1$  except in the following cases.*

- $m = 2$ .
- $q = 2$  and  $m = 4, 6, 12$ .
- $q = 3$  and  $m = 4$ .

*Proof.* This follows immediately from Theorem 3.1.  $\square$

**Corollary 3.5.** *If  $q$  is a prime power and  $m$  is an integer greater than 1, then there exists a Zsigmondy prime  $l \mid q^m - 1$  such that either  $l \geq 3m + 1$  or  $l^2 \mid q^m - 1$  except in the following cases.*

- $m = 2$ .
- $q = 2$  and  $m = 3, 4, 6, 8, 10, 12, 18, 20$ .
- $q = 3$  and  $m = 4$  or  $6$ .
- $q = 4$  and  $m = 3, 6$ .
- $q = 5$  and  $m = 6$ .

*Proof.* This follows immediately from Theorem 3.2.  $\square$

**Corollary 3.6.** *If  $q$  is a prime power and  $m$  is an integer greater than 1, then there exists a prime  $l \mid q^m - 1$  such that either  $l \geq 3m$  or  $l^2 \mid q^m - 1$  and  $l^2 \geq 3m$  except in the following cases.*

- $m = 2$ .
- $q = 2$  and  $m = 3, 4, 6, 8, 12, 20$ .
- $q = 3$  and  $m = 4$  or  $6$ .
- $q = 4$  and  $m = 6$ .

*Proof.* This follows immediately from Theorem 3.2.  $\square$

#### 4. OUTER AUTOMORPHISM OF SIMPLE GROUPS

**Proposition 4.1.** *Let  $G$  be a finite non-abelian simple group. We consider the outer automorphism of  $G$ . We show that there exist two abelian subgroup  $H_1$  and  $H_2$  of  $G$  where  $(|H_1|, |H_2|) = 1$ , and for any subgroup  $K$  of  $\text{Out}(G)$ , we have  $2\sqrt{|K|} \leq |H_i|$ ,  $|K/K'| \leq |H_i|$ ,  $i = 1, 2$ .*

*Proof.* The following elementary fact is used in the proof. Let  $H$  be a group of order  $p^2$ , where  $p$  is a prime, then  $H$  is abelian.

We now go through the classification of the finite simple groups.

- I Alternate groups  $A_n, n \geq 5$ . In general  $|\text{Out}(A_n)| = 2$  except when  $n = 6$  and  $|\text{Out}(A_6)| = 4$ . If  $|\text{Out}(A_n)| = 2$ , then the result is clear since  $4 \mid |A_n|$  and  $3 \mid |A_n|$  when  $n \geq 5$ . When  $n = 6$ ,  $|\text{Out}(A_6)| = 4$  and  $|A_6| = 8 \cdot 9 \cdot 5$  and the result is also clear.
- II Sporadic groups. Thus  $|\text{Out}(G)| \leq 2$  and the result is easy to check.
- III Let  $G$  be of type  $A_1(q)$ ,  $q = p^f$ . We have  $|G| = q(q+1)(q-1)d^{-1}$  where  $d = (2, q-1)$ ,  $|\text{Out}(G)| = df$ . If  $q$  is even, then  $d = 1$  and  $|\text{Out}(G)| \leq f$ . If  $p^{2f} - 1 = (p^f - 1)(p^f + 1)$  has a Zsigmondy prime  $L_1$  and  $p^f - 1$  has a Zsigmondy prime  $L_2$ , then clearly  $L_1 \mid p^{2f} - 1$  and thus  $L_1 \mid p^f + 1$ ,  $L_2 \mid p^f - 1$ ,  $L_1 \neq L_2$  and the result is clear. The exceptional cases are the followings,

- 1)  $f = 1$ , then  $q = 2^1$  and the group  $G$  is solvable.
- 2)  $f = 2$ , then  $q = 2^2$ ,  $|\text{Out}(G)| = 2$ ,  $|G| = 4 \cdot 3 \cdot 5$  and the result is clear.
- 3)  $p = 2$  and  $f = 6$ , thus  $|\text{Out}(G)| = 6$ .  $2^6 - 1 = 9 \cdot 7$  and  $2^6 + 1 = 5 \cdot 13$ .
- 4)  $p = 2$  and  $f = 3$ , thus  $|\text{Out}(G)| = 3$ .  $2^3 - 1 = 7$  and  $2^3 + 1 = 9$ .

If  $q$  is odd, then  $d = 2$  and  $|\text{Out}(G)| \leq 2f$ . If  $p^{2f} - 1 = (p^f - 1)(p^f + 1)$  has a Zsigmondy prime  $L_1$  and  $p^f - 1$  has a prime divisor  $L_2$ , then clearly  $L_1 \mid p^{2f} - 1$  and thus  $L_1 \mid p^f + 1$ ,  $L_2 \mid p^f - 1$ ,  $L_1 \neq L_2$ . It is clear that  $L_1 \geq 2f$ . If  $L_2 \geq 2f$ , then the result is clear. By Corollary 3.4, the exceptional cases are the followings,

- 1)  $f = 1$ , then  $q = p \geq 3$ ,  $|\text{Out}(G)| = 2$ ,  $4 \mid |G|$ ,  $p \mid |G|$  and the result is clear.
- 2)  $f = 2$ , then  $q = p^2 \geq 9$ ,  $|\text{Out}(G)| \leq 4$ ,  $4 \mid |G|$ ,  $p^2 \mid |G|$  and the result is clear.
- 3)  $p = 3$ ,  $f = 4$ ,  $|\text{Out}(G)| \leq 8$ .  $3^4 - 1 = 16 \cdot 5$ ,  $3^4 + 1 = 2 \cdot 41$ . We have 41 and 9 divides  $|G|$ .

- IV Let  $G$  be of type  $A_n(q)$ ,  $q = p^f$ ,  $n \geq 2$ . Set  $m = \prod_{i=1}^n (q^{i+1} - 1)$ . Then  $|G| = d^{-1}q^{n(n+1)/2}m$ ,  $|\text{Out}(G)| = 2fd$  where  $d = (n+1, q-1)$ . By [6, Theorem 3.2], we know that  $\text{Out}(G) \cong D_{2d} \times C_f$  and is not abelian if  $d \geq 3$ .

By Corollary 3.3 and 3.6, we can find Zsigmondy prime  $L_1 \mid p^{f(n+1)} - 1$  and prime  $L_2 \mid p^{fn} - 1$ ,  $L_1 \neq L_2$  such that  $L_1 \geq 2f(n+1)$  or  $L_1^2 \mid p^{f(n+1)} - 1$  which implies that  $L_1^2 \geq 2f(n+1)$  and  $L_2 \geq 3fn \geq 2f(n+1)$  or  $L_2^2 \mid p^{fn} - 1$  and  $L_2^2 \geq 3fn \geq 2f(n+1)$  except for the following cases where  $p$  and  $fn$  are small.

- 1) If  $fn = 2$ , then  $n = 2$ ,  $f = 1$ ,  $p = q$  and  $|\text{Out}(G)| = 2d$  where  $d = (3, q-1)$ .  $|G| = d^{-1}p^3(p^3 - 1)(p^2 - 1)$ . We may pick  $H_1$  such that  $|H_1| = p^2$ . By Corollary 3.3, we may find a Zsigmondy prime  $L \mid p^3 - 1$  such that  $L \geq 6$  or  $L^2 \geq 6$ . And we may pick  $H_2$  where  $|H_2| = L$  or  $|H_2| = L^2$  such that  $|H_2| \geq 6$ .
- 2) If  $p = 2$  and  $fn = 3$ , then  $n = 3$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^3 - 1 = 7$ ,  $2^4 - 1 = 3 \cdot 5$ .
- 3) If  $p = 2$  and  $fn = 4$ , then  $n = 2$ ,  $f = 2$ ,  $q = 4$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 12$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 6$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^6 - 1 = 7 \cdot 9$ .



- 4) If  $p = 2$  and  $fn = 4$ , then  $n = 4$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^5 - 1 = 31$ .
- 5) If  $p = 2$  and  $fn = 6$ , then  $n = 2$ ,  $f = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^6 - 1 = 9 \cdot 7$ ,  $2^9 - 1 = 7 \cdot 73$ .
- 6) If  $p = 2$  and  $fn = 6$ , then  $n = 3$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^6 - 1 = 9 \cdot 7$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ .
- 7) If  $p = 2$  and  $fn = 6$ , then  $n = 6$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^6 - 1 = 9 \cdot 7$ ,  $2^7 - 1 = 127$ .
- 8) If  $p = 2$  and  $fn = 8$ , then  $n = 2$ ,  $f = 4$ ,  $q = 16$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 24$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 12$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 9) If  $p = 2$  and  $fn = 8$ , then  $n = 4$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ .
- 10) If  $p = 2$  and  $fn = 8$ , then  $n = 8$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^9 - 1 = 7 \cdot 73$ .
- 11) If  $p = 2$  and  $fn = 10$ , then  $n = 2$ ,  $f = 5$ ,  $q = 32$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 10$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{15} - 1 = 7 \cdot 31 \cdot 151$ .
- 12) If  $p = 2$  and  $fn = 10$ , then  $n = 5$ ,  $f = 2$ ,  $q = 4$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 13) If  $p = 2$  and  $fn = 10$ , then  $n = 10$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{11} - 1 = 23 \cdot 89$ .
- 14) If  $p = 2$  and  $fn = 12$ , then  $n = 2$ ,  $f = 6$ ,  $q = 64$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 36$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 18$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ .
- 15) If  $p = 2$  and  $fn = 12$ , then  $n = 3$ ,  $f = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$ .
- 16) If  $p = 2$  and  $fn = 12$ , then  $n = 4$ ,  $f = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{15} - 1 = 7 \cdot 31 \cdot 151$ .
- 17) If  $p = 2$  and  $fn = 12$ , then  $n = 6$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{14} - 1 = 3 \cdot 43 \cdot 127$ .
- 18) If  $p = 2$  and  $fn = 12$ , then  $n = 12$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{13} - 1 = 7 \cdot 31 \cdot 8191$ .
- 19) If  $p = 2$  and  $fn = 18$ , then  $n = 2$ ,  $f = 9$ ,  $q = 512$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 18$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{27} - 1 = 7 \cdot 73 \cdot 262654$ .
- 20) If  $p = 2$  and  $fn = 18$ , then  $n = 3$ ,  $f = 6$ ,  $q = 64$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{24} - 1 = 9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ .
- 21) If  $p = 2$  and  $fn = 18$ , then  $n = 6$ ,  $f = 3$ ,  $q = 8$  and  $d = 7$ . Thus  $|\text{Out}(G)| = 42$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{21} - 1 = 49 \cdot 127 \cdot 337$ .
- 22) If  $p = 2$  and  $fn = 18$ , then  $n = 9$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ .
- 23) If  $p = 2$  and  $fn = 18$ , then  $n = 18$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{19} - 1 = 524287$ .
- 24) If  $p = 2$  and  $fn = 20$ , then  $n = 2$ ,  $f = 10$ ,  $q = 1024$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 60$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{30} - 1 = 9 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$ .
- 25) If  $p = 2$  and  $fn = 20$ , then  $n = 4$ ,  $f = 5$ ,  $q = 32$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 10$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{25} - 1 = 31 \cdot 601 \cdot 1801$ .

- 26) If  $p = 2$  and  $fn = 20$ , then  $n = 5$ ,  $f = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{24} - 1 = 9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ .
- 27) If  $p = 2$  and  $fn = 20$ , then  $n = 10$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{22} - 1 = 3 \cdot 23 \cdot 89 \cdot 683$ .
- 28) If  $p = 2$  and  $fn = 20$ , then  $n = 20$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{21} - 1 = 49 \cdot 127 \cdot 337$ .
- 29) If  $p = 3$  and  $fn = 4$ , then  $n = 2$ ,  $f = 2$ ,  $q = 9$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^4 - 1 = 5 \cdot 16$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ .
- 30) If  $p = 3$  and  $fn = 4$ , then  $n = 4$ ,  $f = 1$ ,  $q = 3$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $3^4 - 1 = 5 \cdot 16$ ,  $3^5 - 1 = 2 \cdot 11 \cdot 11$ .
- 31) If  $p = 3$  and  $fn = 6$ , then  $n = 2$ ,  $f = 3$ ,  $q = 27$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^9 - 1 = 2 \cdot 13 \cdot 757$ .
- 32) If  $p = 3$  and  $fn = 6$ , then  $n = 3$ ,  $f = 2$ ,  $q = 9$  and  $d = 4$ . Thus  $|\text{Out}(G)| = 16$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 8$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^8 - 1 = 32 \cdot 5 \cdot 41$ .
- 33) If  $p = 3$  and  $fn = 6$ , then  $n = 6$ ,  $f = 1$ ,  $q = 3$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^7 - 1 = 2 \cdot 1093$ .
- 34) If  $p = 5$  and  $fn = 6$ , then  $n = 2$ ,  $f = 3$ ,  $q = 125$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^9 - 1 = 4 \cdot 19 \cdot 31 \cdot 829$ .
- 35) If  $p = 5$  and  $fn = 6$ , then  $n = 3$ ,  $f = 2$ ,  $q = 25$  and  $d = 4$ . Thus  $|\text{Out}(G)| = 16$  (not abelian),  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^8 - 1 = 32 \cdot 3 \cdot 13 \cdot 313$ .
- 36) If  $p = 5$  and  $fn = 6$ , then  $n = 6$ ,  $f = 1$ ,  $q = 5$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^7 - 1 = 4 \cdot 19531$ .
- 37)  $p = 2$  and  $f(n+1) = 4$ , then  $n+1 = 4$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^3 - 1 = 7$ ,  $2^4 - 1 = 3 \cdot 5$ .
- 38)  $p = 2$  and  $f(n+1) = 6$ , then  $n+1 = 3$ ,  $f = 2$ ,  $q = 4$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 12$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 6$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^6 - 1 = 7 \cdot 9$ .
- 39)  $p = 2$  and  $f(n+1) = 6$ , then  $n+1 = 6$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^5 - 1 = 31$ .
- 40)  $p = 2$  and  $f(n+1) = 12$ , then  $n+1 = 3$ ,  $f = 4$ ,  $q = 16$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 24$  and  $\text{Out}(G)$  is not abelian,  $|K/K'| \leq 12$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ .
- 41)  $p = 2$  and  $f(n+1) = 12$ , then  $n+1 = 4$ ,  $f = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^9 - 1 = 7 \cdot 73$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 42)  $p = 2$  and  $f(n+1) = 12$ , then  $n+1 = 6$ ,  $f = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 43)  $p = 2$  and  $f(n+1) = 12$ , then  $n+1 = 12$ ,  $f = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{11} - 1 = 23 \cdot 89$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 44)  $p = 3$  and  $f(n+1) = 4$ , then  $n+1 = 4$ ,  $f = 1$ ,  $q = 3$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^3 - 1 = 2 \cdot 13$ ,  $3^4 - 1 = 16 \cdot 5$ .
- 45)  $p = 3$  and  $f(n+1) = 6$ , then  $n+1 = 3$ ,  $f = 2$ ,  $q = 9$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^4 - 1 = 16 \cdot 5$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ .
- 46)  $p = 3$  and  $f(n+1) = 6$ , then  $n+1 = 6$ ,  $f = 1$ ,  $q = 3$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^5 - 1 = 2 \cdot 11 \cdot 11$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ .

When  $q = 2$ ,  $d = 1$ ,  $f = 1$  and the result is easy to check.  $q^{n+1} - 1$ ,  $q^n - 1$ .

When  $q = 3$ ,  $d \leq 2$ ,  $f = 1$  and the result is easy to check.  $q^{n+1} - 1$ ,  $q^n - 1$ .

- V Let  $G$  be of type  $B_n(q)$ ,  $n \geq 2$ ,  $q = p^f$ . Set  $m = \prod_{i=1}^n (q^{2^i} - 1)$ . Then  $|G| = d^{-1}q^{n^2}m$ ,  $|\text{Out}(G)| = df$ , where  $d = (2, q - 1)$ ,  $g = 1$  unless  $n = p = g = 2$ . Thus  $|\text{Out}(G)| \leq 2f$ . By Corollary 3.3, we can find Zsigmondy prime  $L_1 \mid p^{f(2n)} - 1$  and Zsigmondy prime  $L_2 \mid p^{f(2n-2)} - 1$  such that  $L_1 \geq 2f$  or  $L_1^2 \mid p^{f(2n)} - 1$  which implies that  $L_1^2 \geq 2f$  and  $L_2 \geq 2f$  or  $L_2^2 \mid p^{f(2n-2)} - 1$  which implies that  $L_2^2 \geq 2f$  except for the following cases where  $p$  and  $fn$  are small.
- 1) If  $f(2n - 2) = 2$ , then  $f = 1$  and  $n = 2$ . Thus  $p^{f(2n)} - 1$  will have a Zsigmondy prime and it is clear that  $p^{f(2n-2)} - 1 = p^2 - 1$  will have a different prime divisor  $\geq 2$ .
  - 2) If  $p = 2$  and  $f(2n - 2) = 6$ , then either  $2n - 2 = 2$  and  $f = 3$ , in this case  $2f = 6$ ,  $p^{f(2n)} - 1 = 2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$  and  $p^{f(2n-2)} - 1 = 2^6 - 1 = 7 \cdot 9$ , we can pick  $|H_1| = 13$  and  $|H_2| = 7$ ; or  $2n - 2 = 3$  and  $f = 2$ , in this case  $2f = 4$ ,  $p^{f(2n)} - 1 = 2^{10} - 1 = 3 \cdot 11 \cdot 31$  and  $p^{f(2n-2)} - 1 = 2^6 - 1 = 7 \cdot 9$ , we can pick  $|H_1| = 11$  and  $|H_2| = 7$ .
  - 3) If  $p = 2$  and  $f(2n) = 6$ , then  $n = 3$  and  $f = 1$ , in this case  $2f = 2$ ,  $p^{f(2n)} - 1 = 2^6 - 1 = 7 \cdot 9$  and  $p^{f(2n-2)} - 1 = 2^4 - 1 = 3 \cdot 5$ , we can pick  $|H_1| = 7$  and  $|H_2| = 5$ .
- VI Let  $G$  be of type  $C_n(q)$ ,  $n \geq 3$ ,  $q = p^f$ . Set  $m = \prod_{i=1}^n (q^{2^i} - 1)$ . Then  $|G| = d^{-1}q^{n^2}m$ ,  $|\text{Out}(G)| = df$ , where  $d = (2, q - 1)$ . Thus  $|\text{Out}(G)| \leq 2f$ . By Corollary 3.3, we can find Zsigmondy prime  $L_1 \mid p^{f(2n)} - 1$  and Zsigmondy prime  $L_2 \mid p^{f(2n-2)} - 1$  such that  $L_1 \geq 2f$  or  $L_1^2 \mid p^{f(2n)} - 1$  which implies that  $L_1^2 \geq 2f$  and  $L_2 \geq 2f$  or  $L_2^2 \mid p^{f(2n-2)} - 1$  which implies that  $L_2^2 \geq 2f$  except for a few cases where  $p$  and  $fn$  are small. The proof is similar to the previous case.
- VII Let  $G$  be of type  $D_n(q)$ ,  $n \geq 4$ ,  $q = p^f$ . Set  $m = \prod_{i=1}^{n-1} (q^{2^i} - 1)$ . Then  $|G| = d^{-1}q^{n(n-1)}(q^n - 1)m$ ,  $|\text{Out}(G)| = (2, q - 1)^2 \cdot f \cdot S_3$  for  $n = 4$ ,  $(2, q - 1)^2 \cdot f \cdot 2$  for  $n > 4$  even,  $(4, q^n - 1) \cdot f \cdot 2$  for  $n$  odd.
- When  $n \geq 5$ ,  $|\text{Out}(G)| \leq 8f$ . Since  $2n - 2 \geq 8$ ,  $p^{f(2n-2)} - 1$  will always have a Zsigmondy prime  $L_1 \geq 8f$ . By Corollary 3.4,  $p^{f(2n-4)} - 1$  will have a prime divisor  $L_2$  such that  $L_2 \geq 12f$  or  $L_2^2 \mid p^{f(2n-4)} - 1$  and  $L_2^2 \geq 12f$  except for the following cases,
- 1)  $p = 2$ ,  $2n - 4 = 6$  and  $f = 1$ . Thus  $|\text{Out}(G)| \leq 8f = 8$  and  $2^6 - 1 = 7 \cdot 9$ .
  - 2)  $p = 2$ ,  $2n - 4 = 6$  and  $f = 2$ . Thus  $|\text{Out}(G)| \leq 8f = 16$  and  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .  $p^{f(2n-2)} = 2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$ . In this case, we have 17 and 257 divide  $|G|$ .
  - 3)  $p = 2$ ,  $2n - 4 = 12$  and  $f = 1$ . Thus  $|\text{Out}(G)| \leq 8f = 8$  and  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- When  $n = 4$  and  $q$  is even,  $(2, q - 1) = 1$ .  $|\text{Out}(G)| \leq 6f$  and  $|\text{Out}(G)/\text{Out}(G)'| \leq 3f$  since  $S_3$  is not abelian. We have  $q^{2n-2} - 1 = 2^{6f} - 1$ ,  $q^{2n-4} - 1 = 2^{4f} - 1$ .  $2^{6f} - 1$  will always have a Zsigmondy prime  $L_1 \geq 6f$ . By Corollary 3.3,  $2^{4f} - 1$  will have a Zsigmondy prime  $L_2 \geq 8f$  except for the following cases,
- 1)  $f = 1$ .  $|\text{Out}(G)| \leq 6$  and  $|\text{Out}(G)/\text{Out}(G)'| \leq 3$ . Thus  $2^6 - 1 = 9 \cdot 7$  and  $2^4 - 1 = 3 \cdot 5$ .  $9 \mid |G|$  and  $5 \mid |G|$ .
  - 2)  $f = 3$ .  $|\text{Out}(G)| \leq 18$  and  $|\text{Out}(G)/\text{Out}(G)'| \leq 9$ . Thus  $2^{18} - 1 = 7 \cdot 7 \cdot 19 \cdot 73$  and  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .  $19 \mid |G|$  and  $73 \mid |G|$ .
- When  $n = 4$  and  $q$  is odd,  $(2, q - 1) = 2$  and thus  $|\text{Out}(G)| \leq 24f$  and  $|\text{Out}(G)/\text{Out}(G)'| \leq 12f$  since  $S_3$  is not abelian. We have  $q^{2n-2} - 1 = p^{6f} - 1$ ,  $q^{2n-4} - 1 = p^{4f} - 1$ . By Corollary 3.3 and 3.5, we can find Zsigmondy prime  $L_1 \mid p^{6f} - 1$  and Zsigmondy prime  $L_2 \mid p^{4f} - 1$  such that  $L_1 \geq 12f$  or  $L_1^2 \mid p^{6f} - 1$  which implies that  $L_1^2 \geq 12f$  and  $L_2 \geq 12f$  or  $L_2^2 \mid p^{4f} - 1$  which implies that  $L_2^2 \geq 12f$  except for the following cases where  $p$  and  $fn$  are small.

- 1)  $p = 3$ ,  $6f = 6$  and  $f = 1$ .  $|\text{Out}(G)/\text{Out}(G)'| \leq 12$ . Thus  $3^6 - 1 = 8 \cdot 7 \cdot 13$  and  $3^4 - 1 = 16 \cdot 5$ .  $13 \mid |G|$  and  $25 \mid |G|$ .
  - 2)  $p = 5$ ,  $6f = 6$  and  $f = 1$ .  $|\text{Out}(G)/\text{Out}(G)'| \leq 12$ . Thus  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$  and  $5^4 - 1 = 16 \cdot 3 \cdot 13$ .
- VIII Let  $G$  be of type  ${}^2A_n(q^2)$ ,  $n \geq 2$ . Note that if  $n = 2$ , then  $q > 2$ . Set  $m = \prod_{i=1}^n (q^{i+1} - (-1)^{i+1})$ ,  $q^2 = p^f$ , and  $d = (n+1, q+1)$ . Then  $|G| = d^{-1}mq^{n(n+1)/2}$ ,  $|\text{Out}(G)| = d \cdot f$ . By Corollary 3.3 and 3.5, we can find Zsigmondy prime  $L_1 \mid p^{f(n+1)/2} - (-1)^{n+1}$  and Zsigmondy prime  $L_2 \mid p^{fn/2} - (-1)^n$  such that  $L_1 \geq (n+1)f$  or  $L_1^2 \mid p^{f(n+1)/2} - (-1)^{n+1}$  which implies that  $L_1^2 \geq (n+1)f$  and  $L_2 \geq (n+1)f$  or  $L_2^2 \mid p^{fn/2} - (-1)^n$  which implies that  $L_2 \geq 3(fn/2) \geq (n+1)f$  except for a few cases where  $p$  and  $fn$  are small.
- 1) If  $fn/2 = 2$ , then  $n = 2$ ,  $f = 2$ ,  $p = q$  and  $|\text{Out}(G)| = 2d$  where  $d = (3, p+1)$ .  $|G| = d^{-1}p^3(p^3 + 1)(p^2 - 1)$ . We may pick  $H_1$  such that  $|H_1| = p^2$ . We may find a Zsigmondy prime  $L \mid p^6 - 1$  such that  $L \mid p^3 + 1$  and  $L \geq 6$ . And we may pick  $H_2$  such that  $|H_2| = L$ .
  - 2) If  $p = 2$  and  $fn/2 = 3$ , then  $n = 3$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^3 + 1 = 9$ ,  $2^4 - 1 = 3 \cdot 5$ .
  - 3) If  $p = 2$  and  $fn/2 = 4$ , then  $n = 2$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^6 + 1 = 5 \cdot 13$ .
  - 4) If  $p = 2$  and  $fn/2 = 4$ , then  $n = 4$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^5 + 1 = 3 \cdot 11$ .
  - 5) If  $p = 2$  and  $fn/2 = 6$ , then  $n = 2$ ,  $f/2 = 3$ ,  $q = 8$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 18$  and  $\text{Out}(G)$  is not abelian (by GAP),  $|K/K'| \leq 9$ ,  $2^6 - 1 = 7 \cdot 9$ ,  $2^9 + 1 = 27 \cdot 19$ .
  - 6) If  $p = 2$  and  $fn/2 = 6$ , then  $n = 3$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^6 + 1 = 5 \cdot 13$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ .
  - 7) If  $p = 2$  and  $fn/2 = 6$ , then  $n = 6$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^6 - 1 = 7 \cdot 9$ ,  $2^7 + 1 = 3 \cdot 43$ .
  - 8) If  $p = 2$  and  $fn/2 = 8$ , then  $n = 2$ ,  $f/2 = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^{12} + 1 = 17 \cdot 241$ .
  - 9) If  $p = 2$  and  $fn/2 = 8$ , then  $n = 4$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 5$ . Thus  $|\text{Out}(G)| = 20$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^{10} + 1 = 25 \cdot 41$ .
  - 10) If  $p = 2$  and  $fn/2 = 8$ , then  $n = 8$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^9 + 1 = 27 \cdot 19$ .
  - 11) If  $p = 2$  and  $fn/2 = 10$ , then  $n = 2$ ,  $f/2 = 5$ ,  $q = 32$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 30$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{15} + 1 = 9 \cdot 11 \cdot 331$ .
  - 12) If  $p = 2$  and  $fn/2 = 10$ , then  $n = 5$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{10} + 1 = 25 \cdot 41$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
  - 13) If  $p = 2$  and  $fn/2 = 10$ , then  $n = 10$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ ,  $2^{11} + 1 = 3 \cdot 683$ .
  - 14) If  $p = 2$  and  $fn/2 = 12$ , then  $n = 2$ ,  $f/2 = 6$ ,  $q = 64$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$ .
  - 15) If  $p = 2$  and  $fn/2 = 12$ , then  $n = 3$ ,  $f/2 = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^{12} + 1 = 17 \cdot 241$ ,  $2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$ .
  - 16) If  $p = 2$  and  $fn/2 = 12$ , then  $n = 4$ ,  $f/2 = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{15} + 1 = 9 \cdot 11 \cdot 331$ .

- 17) If  $p = 2$  and  $fn/2 = 12$ , then  $n = 6$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{14} + 1 = 5 \cdot 29 \cdot 113$ .
- 18) If  $p = 2$  and  $fn/2 = 12$ , then  $n = 12$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{13} + 1 = 3 \cdot 2731$ .
- 19) If  $p = 2$  and  $fn/2 = 18$ , then  $n = 2$ ,  $f/2 = 9$ ,  $q = 512$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 54$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{27} + 1 = 81 \cdot 19 \cdot 87211$ .
- 20) If  $p = 2$  and  $fn/2 = 18$ , then  $n = 3$ ,  $f/2 = 6$ ,  $q = 64$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$ ,  $2^{24} - 1 = 9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ .
- 21) If  $p = 2$  and  $fn/2 = 18$ , then  $n = 6$ ,  $f/2 = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{21} + 1 = 9 \cdot 43 \cdot 5419$ .
- 22) If  $p = 2$  and  $fn/2 = 18$ , then  $n = 9$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 5$ . Thus  $|\text{Out}(G)| = 20$ ,  $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ .
- 23) If  $p = 2$  and  $fn/2 = 18$ , then  $n = 18$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ ,  $2^{19} + 1 = 3 \cdot 174763$ .
- 24) If  $p = 2$  and  $fn/2 = 20$ , then  $n = 2$ ,  $f/2 = 10$ ,  $q = 1024$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 20$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{30} + 1 = 25 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$ .
- 25) If  $p = 2$  and  $fn/2 = 20$ , then  $n = 4$ ,  $f/2 = 5$ ,  $q = 32$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 10$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{25} + 1 = 3 \cdot 11 \cdot 251 \cdot 4051$ .
- 26) If  $p = 2$  and  $fn/2 = 20$ , then  $n = 5$ ,  $f/2 = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^{20} + 1 = 17 \cdot 61681$ ,  $2^{24} - 1 = 9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ .
- 27) If  $p = 2$  and  $fn/2 = 20$ , then  $n = 10$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{22} + 1 = 5 \cdot 397 \cdot 2113$ .
- 28) If  $p = 2$  and  $fn/2 = 20$ , then  $n = 20$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{20} - 1 = 3 \cdot 25 \cdot 11 \cdot 31 \cdot 41$ ,  $2^{21} + 1 = 9 \cdot 43 \cdot 5419$ .
- 29) If  $p = 3$  and  $fn/2 = 4$ , then  $n = 2$ ,  $f/2 = 2$ ,  $q = 9$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^4 - 1 = 5 \cdot 16$ ,  $3^6 + 1 = 2 \cdot 5 \cdot 73$ .
- 30) If  $p = 3$  and  $fn/2 = 4$ , then  $n = 4$ ,  $f/2 = 1$ ,  $q = 3$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $3^4 - 1 = 5 \cdot 16$ ,  $3^5 + 1 = 4 \cdot 61$ .
- 31) If  $p = 3$  and  $fn/2 = 6$ , then  $n = 2$ ,  $f/2 = 3$ ,  $q = 27$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^9 + 1 = 4 \cdot 7 \cdot 19 \cdot 37$ .
- 32) If  $p = 3$  and  $fn/2 = 6$ , then  $n = 3$ ,  $f/2 = 2$ ,  $q = 9$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 8$ ,  $3^6 + 1 = 2 \cdot 5 \cdot 73$ ,  $3^8 - 1 = 32 \cdot 5 \cdot 41$ .
- 33) If  $p = 3$  and  $fn/2 = 6$ , then  $n = 6$ ,  $f/2 = 1$ ,  $q = 3$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^7 + 1 = 4 \cdot 547$ .
- 34) If  $p = 5$  and  $fn/2 = 6$ , then  $n = 2$ ,  $f/2 = 3$ ,  $q = 125$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 18$ ,  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^9 + 1 = 2 \cdot 27 \cdot 7 \cdot 5167$ .
- 35) If  $p = 5$  and  $fn/2 = 6$ , then  $n = 3$ ,  $f/2 = 2$ ,  $q = 25$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 8$ ,  $5^6 + 1 = 2 \cdot 13 \cdot 601$ ,  $5^8 - 1 = 32 \cdot 3 \cdot 13 \cdot 313$ .
- 36) If  $p = 5$  and  $fn/2 = 6$ , then  $n = 6$ ,  $f/2 = 1$ ,  $q = 5$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^7 + 1 = 2 \cdot 3 \cdot 29 \cdot 449$ .
- 37)  $p = 2$  and  $f(n+1)/2 = 4$ , then  $n+1 = 4$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^3 + 1 = 9$ ,  $2^4 - 1 = 3 \cdot 5$ .
- 38)  $p = 2$  and  $f(n+1)/2 = 6$ , then  $n+1 = 3$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^4 - 1 = 3 \cdot 5$ ,  $2^6 + 1 = 5 \cdot 13$ .

- 39)  $p = 2$  and  $f(n+1)/2 = 6$ , then  $n+1 = 6$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^5 + 1 = 3 \cdot 11$ ,  $2^6 - 1 = 7 \cdot 9$ .
- 40)  $p = 2$  and  $f(n+1)/2 = 10$ , then  $n+1 = 5$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 5$ . Thus  $|\text{Out}(G)| = 20$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ ,  $2^{10} + 1 = 25 \cdot 41$ .
- 41)  $p = 2$  and  $f(n+1)/2 = 10$ , then  $n+1 = 10$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 2$ ,  $2^9 + 1 = 27 \cdot 19$ ,  $2^{10} - 1 = 3 \cdot 11 \cdot 31$ .
- 42)  $p = 2$  and  $f(n+1)/2 = 12$ , then  $n+1 = 3$ ,  $f/2 = 4$ ,  $q = 16$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 8$ ,  $2^{12} + 1 = 17 \cdot 241$ ,  $2^8 - 1 = 3 \cdot 5 \cdot 17$ .
- 43)  $p = 2$  and  $f(n+1)/2 = 12$ , then  $n+1 = 4$ ,  $f/2 = 3$ ,  $q = 8$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^9 + 1 = 27 \cdot 19$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 44)  $p = 2$  and  $f(n+1)/2 = 12$ , then  $n+1 = 6$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{10} + 1 = 25 \cdot 41$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 45)  $p = 2$  and  $f(n+1)/2 = 12$ , then  $n+1 = 12$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^{11} + 1 = 3 \cdot 683$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ .
- 46)  $p = 2$  and  $f(n+1)/2 = 18$ , then  $n+1 = 3$ ,  $f/2 = 6$ ,  $q = 64$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 12$ ,  $2^{12} - 1 = 9 \cdot 5 \cdot 7 \cdot 13$ ,  $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$ .
- 47)  $p = 2$  and  $f(n+1)/2 = 18$ , then  $n+1 = 6$ ,  $f/2 = 3$ ,  $q = 8$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 18$ ,  $2^{15} + 1 = 9 \cdot 11 \cdot 331$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ .
- 48)  $p = 2$  and  $f(n+1)/2 = 18$ , then  $n+1 = 9$ ,  $f/2 = 2$ ,  $q = 4$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$ ,  $2^{18} + 1 = 5 \cdot 13 \cdot 37 \cdot 109$ .
- 49)  $p = 2$  and  $f(n+1)/2 = 18$ , then  $n+1 = 18$ ,  $f/2 = 1$ ,  $q = 2$  and  $d = 3$ . Thus  $|\text{Out}(G)| = 6$ ,  $2^{17} + 1 = 3 \cdot 43691$ ,  $2^{18} - 1 = 27 \cdot 7 \cdot 19 \cdot 73$ .
- 50)  $p = 3$  and  $f(n+1)/2 = 4$ , then  $n+1 = 4$ ,  $f/2 = 1$ ,  $q = 3$  and  $d = 4$ . Thus  $|\text{Out}(G)| = 8$  and  $\text{Out}(G)$  is not abelian (the outer automorphism of  $\text{PSU}(4, 3)$  is not abelian by GAP),  $|K/K'| \leq 4$ ,  $3^3 + 1 = 4 \cdot 7$ ,  $3^4 - 1 = 16 \cdot 5$ .
- 51)  $p = 3$  and  $f(n+1)/2 = 6$ , then  $n+1 = 3$ ,  $f/2 = 2$ ,  $q = 9$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^4 - 1 = 16 \cdot 5$ ,  $3^6 + 1 = 2 \cdot 5 \cdot 73$ .
- 52)  $p = 3$  and  $f(n+1)/2 = 6$ , then  $n+1 = 6$ ,  $f/2 = 1$ ,  $q = 3$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^5 + 1 = 4 \cdot 61$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ .
- 53)  $p = 5$  and  $f(n+1)/2 = 6$ , then  $n+1 = 3$ ,  $f/2 = 2$ ,  $q = 25$  and  $d = 1$ . Thus  $|\text{Out}(G)| = 4$ ,  $5^4 - 1 = 16 \cdot 3 \cdot 13$ ,  $5^6 + 1 = 2 \cdot 13 \cdot 601$ .
- 54)  $p = 5$  and  $f(n+1)/2 = 6$ , then  $n+1 = 6$ ,  $f/2 = 1$ ,  $q = 5$  and  $d = 6$ . Thus  $|\text{Out}(G)| = 12$ ,  $5^5 + 1 = 2 \cdot 3 \cdot 521$ ,  $5^6 - 1 = 8 \cdot 7 \cdot 9 \cdot 31$ .
- IX Let  $G$  be of type  ${}^2D_n(q^2)$ ,  $n \geq 4$ . Set  $m = \prod_{i=1}^{n-1} (q^{2i} - 1)$ ,  $q^2 = p^f$ , and  $d = (4, q^n + 1)$ . Then  $|G| = d^{-1} m q^{n(n-1)} (q^n + 1)$ ,  $|\text{Out}(G)| = (4, q^n + 1) \cdot f \leq 4f$ . By Corollary 3.3 and 3.4, we can find Zsigmondy prime  $L_1 \mid p^{f(n-1)} - 1$  such that  $L_1 \geq 4f$  or  $L_1^2 \mid p^{f(n-1)} - 1$  which implies that  $L_1^2 \geq 4f$ , and prime  $L_2 \mid p^{f(n-2)} - 1$  such that  $L_2 \geq 4f$  or  $L_2^2 \mid p^{f(n-2)} - 1$  and  $L_2^2 \geq 4f$  except for the following cases where  $p$  and  $fn$  are small.
- $p^{f(n-1)} - 1$ ,  $p^{f(n-2)} - 1$ . If  $q$  is even, only  $f$  and it is easy, we may assume  $q$  is odd.
- $n - 1 \geq 3$  and  $n - 2 \geq 2$ .  $2 \mid f$
- 1)  $p = 3$  and  $f(n-1) = 6$ , then  $n-1 = 3$ ,  $f = 2$ ,  $q = 3$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^4 - 1 = 16 \cdot 5$ .
- 2)  $p = 5$  and  $f(n-1) = 6$ , then  $n-1 = 3$ ,  $f = 2$ ,  $q = 5$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $5^6 - 1 = 8 \cdot 9 \cdot 7 \cdot 31$ ,  $5^4 - 1 = 16 \cdot 3 \cdot 13$ .

3)  $p = 3$  and  $f(n - 2) = 4$ , then  $n - 2 = 2$ ,  $f = 2$ ,  $q = 3$  and  $d = 2$ . Thus  $|\text{Out}(G)| = 4$ ,  $3^6 - 1 = 8 \cdot 7 \cdot 13$ ,  $3^4 - 1 = 5 \cdot 16$ .

X Let  $G$  be one of the following types:

$E_6(q)$ ,  $|G| = q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1)/(3, q - 1)$  where  $q = p^f$ .  $|\text{Out}(G)| = (3, q - 1) \cdot f \cdot 2$ .  $q^{12} - 1$  and  $q^8 - 1$  always have Zsigmondy primes.

$E_7(q)$ ,  $|G| = q^{63}(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^{10} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)/(2, q - 1)$  where  $q = p^f$ .  $|\text{Out}(G)| = (2, q - 1) \cdot f$ .  $q^{18} - 1$  and  $q^{14} - 1$  always have Zsigmondy primes.

$E_8(q)$ ,  $|G| = q^{120}(q^{30} - 1)(q^{24} - 1)(q^{20} - 1)(q^{18} - 1)(q^{14} - 1)(q^{12} - 1)(q^8 - 1)(q^2 - 1)$  where  $q = p^f$ .  $|\text{Out}(G)| = f$ .  $q^{30} - 1$  and  $q^{24} - 1$  always have Zsigmondy primes.

$F_4(q)$ ,  $|G| = q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)$  where  $q = p^f$ .  $|\text{Out}(G)| = f$  for  $q$  odd and  $|\text{Out}(G)| = 2 \cdot f$  for  $q$  even.  $q^{12} - 1$  and  $q^8 - 1$  always have Zsigmondy primes.

$G_2(q)$ ,  $|G| = q^6(q^6 - 1)(q^2 - 1)$  where  $q = p^f$ .  $|\text{Out}(G)| = f$  for  $q$  not a power of 3 and  $|\text{Out}(G)| = 2 \cdot f$  for  $q$  a power of 3.  $q^6 - 1 = p^{6f} - 1$  always has a Zsigmondy prime  $L_1$  such that  $L_1 \geq 6f$  except for when  $p = 2$  and  $f = 1$ , and in this case  $q^6 - 1 = 2^6 - 1 = 7 \cdot 9$ .  $q^2 - 1 = p^{2f} - 1$  always has a Zsigmondy prime  $L_2$  such that  $L_2 \geq 2f$  except for when  $p = 2$  and  $f = 3$ , and in this case  $q^6 - 1 = 2^6 - 1 = 7 \cdot 9$  or  $f = 1$  and the result is clear.

${}^2E_6(q^2)$ ,  $|G| = q^{36}(q^{12} - 1)(q^9 + 1)(q^8 - 1)(q^6 - 1)(q^5 + 1)(q^2 - 1)/(3, q + 1)$  where  $q^2 = p^f$ .  $|\text{Out}(G)| = (3, q + 1) \cdot f$ .  $q^{12} - 1$  and  $q^8 - 1$  always have Zsigmondy primes.

${}^3D_4(q^3)$ ,  $|G| = q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$  where  $q^3 = p^f$ .  $3 \mid f$  and  $|\text{Out}(G)| = f$ .  $q^{12} - 1 = p^{4f} - 1$  has a Zsigmondy prime  $L_1$  such that  $L_1 \geq 4f$ .  $q^6 - 1 = p^{2f} - 1$  always has a Zsigmondy prime  $L_2$  such that  $L_2 \geq 2f$  except for when  $p = 2$  and  $f = 3$ , and in this case  $q^6 - 1 = 2^6 - 1 = 7 \cdot 9$ .

XI Let  $G$  be of type  ${}^2B_2(2^{2n+1})$ ,  $n \geq 1$ . Then  $|G| = q^2(q^2 + 1)(q - 1)$  where  $q = 2^{2n+1}$ ,  $|\text{Out}(G)| = 2n + 1$ .  $q^2 + 1$  and  $q - 1$  always have Zsigmondy primes.

XII Let  $G$  be Ree groups of type  ${}^2F_4(2^{2n+1})$ ,  $n \geq 1$ . Then  $|G| = q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1)$  where  $q = 2^{2n+1}$ ,  $|\text{Out}(G)| = 2n + 1$ .  $q^4 - 1$  and  $q - 1$  always have Zsigmondy primes.

XIII Tits group has  $|\text{Out}(G)| = 2$  and the result is clear.

XIV Let  $G$  be Ree groups of type  ${}^2G_2(3^{2n+1})$ ,  $n \geq 1$ . Then  $|G| = q^3(q^3 + 1)(q - 1)$  where  $q = 3^{2n+1}$ ,  $|\text{Out}(G)| = 2n + 1$ .  $q^3 + 1$  and  $q - 1$  always have Zsigmondy primes.

□

The following two corollaries follow immediately from Proposition 4.1.

**Corollary 4.2.** *Let  $G$  be a finite simple group and  $p$  be a fixed prime. Let  $\text{Out}(G)$  denote the outer automorphism of  $G$ . Then there exist an abelian subgroup  $H$  of  $G$  where  $(|H|, p) = 1$  and  $2\sqrt{|\text{Out}(G)|} \leq |H|$ .*

**Corollary 4.3.** *Let  $G$  be a finite simple group and  $p$  be a fixed prime. Let  $\text{Out}(G)$  denote the outer automorphism of  $G$ . Then there exist an abelian subgroup  $H$  of  $G$  where  $(|H|, p) = 1$  and for any subgroup  $K$  of  $\text{Out}(G)$ ,  $|K/K'| \leq |H|$ .*

**Proposition 4.4.** *Let  $p$  be a fixed prime. Assume that  $N \triangleleft G$  where  $N = L_1 \times \cdots \times L_m$  be the product of  $m$  finite non-abelian simple groups  $L_i$  permuted transitively by  $G$ . Let  $K = \bigcap_i \mathbf{N}_G(L_i)$ . Clearly  $K/N \leq \text{Out}L_1 \times \cdots \times \text{Out}L_m$ . Then there exists an abelian subgroup  $H = H_1 \times \cdots \times H_m$  where  $H_i \subset L_i$ ,  $(|H|, p) = 1$  and  $|G/G'| \leq |H|$ .*

*Proof.* If  $m = 1$ , then  $G/N$  is a subgroup of  $\text{Out}(L_1)$ . There exists an abelian group  $H_1 \subset L_1$  such that  $|G : G'| \leq |G/N : (G/N)'| \leq |H_1|$  and  $(|H_1|, p) = 1$  by Corollary 4.3.

Assume  $X = X_1 \times \cdots \times X_m$ ,  $m > 1$ , be the direct product of finite groups  $X_i$  permuted transitively by  $G$ . If  $V$  is a  $G$ -invariant subgroup of  $X$ , then  $|V : [G, V]| \leq |X|^{1/2}$ . Proof. Choose  $g \in G$  that leaves no  $X_i$  invariant. Then  $|C_X(g)| \leq |X|^{1/2}$ . Hence  $|V : [G, V]| \leq |V : [g, V]| \leq |C_V(g)| \leq |C_X(g)| \leq |X|^{1/2}$ .

If  $m > 1$ , then  $K/N$  is a  $G$ -invariant subgroup of  $\text{Out}L_1 \times \cdots \times \text{Out}L_m$ . Thus  $|K/N : [G, K/N]| \leq |\text{Out}(L_1)|^{m/2}$  by the previous paragraph. Thus  $|G/G'| = |G : G'K| |K : K \cap G'| \leq 2^{m-1} |\text{Out}(L_1)|^{m/2}$  by [1, Theorem 2]. There exists an abelian subgroup  $H = H_1 \times \cdots \times H_m$  where  $H_i \subset L_i$ ,  $(|H|, p) = 1$  and  $|G/G'| \leq |H|$  by Corollary 4.2.  $\square$

## 5. REDUCTION TO $Z = 1$

In this section we finally prove Theorem 1.1.

**Theorem 5.1.** *Let  $G$  be a finite group and  $V$  a finite faithful completely reducible  $G$ -module, possibly of mixed characteristic. Let  $M$  be the largest orbit size in the action of  $G$  on  $V$ . Then*

$$|G/G'| \leq M.$$

*Proof.* Suppose that  $G, V$  is a counterexample such that  $|GV|$  is minimal. First observe that with the same arguments used in the proof of [5, Theorem 2.3] we may assume that  $V$  is irreducible. Let  $p$  be the characteristic of  $V$ . Then clearly  $O_p(G) = 1$ .

Let  $Z = Z(E(G))$ . By the proof of [4, Lemma 3.15] and by [4, Lemma 3.16] we know that  $F(G/Z) = F(G)/Z$ ,  $E(G/Z) = E(G)/Z$ ,  $F^*(G/Z) = F^*(G)/Z$ , and  $C_{G/Z}(E(G/Z)) = C_G(E(G))/Z$ .

We work in  $\bar{G} = G/Z$  and put  $\bar{C} = C_{\bar{G}}(E(\bar{G})) = C_G(E(G))/Z$ .

By Corollary 2.4 we have

$$|\bar{C} : \bar{C}'| \leq |F(\bar{G}) : F(\bar{G})'|$$

$E(G)/Z = E_1 \times E_2 \times \cdots \times E_n$  where  $E(G)/Z$  is a direct product of simple groups.

Consider  $K = \bar{G}/\bar{C}$ ,  $K$  acts faithfully on  $E(G)/Z$ . We may assume that  $K_0 = K$  acts transitively on  $L_1 = E_{11} \times E_{12} \times \cdots \times E_{1m_1}$ . Let  $K_1 = \mathbf{C}_K(L_1)$ . We may assume that  $K_1$  acts transitively on  $L_2 = E_{21} \times E_{22} \times \cdots \times E_{2m_2}$  and let  $K_2 = \mathbf{C}_{K_1}(L_2)$ . Inductively, we may define  $L_3, K_3 \dots L_t, K_t$ .

Clearly  $E(G)/Z = L_1 \times L_2 \cdots \times L_t$  and we know that  $K_{i-1}/K_i$  acts transitively and faithfully on  $L_i$  where  $i = 1, \dots, t$ .

By Proposition 4.4, there exists an abelian group  $A_i$  where  $A_i \subset L_i$ ,  $(|A_i|, p) = 1$  and  $|K_{i-1}/K_i : (K_{i-1}/K_i)'| \leq |A_i|$  for  $1 \leq i \leq t$ .

Let  $\bar{A} = A_1 \times \cdots \times A_t$ , thus  $\bar{A}$  is abelian,  $(|\bar{A}|, p) = 1$  and  $|K : K'| \leq |\bar{A}|$ .

Hence altogether we have

$$|\bar{G} : \bar{G}'| \leq |K : K'| |\bar{C} : \bar{C}'| \leq |\bar{A}| |F(\bar{G}) : F(\bar{G})'|, \quad (1)$$

and as  $\bar{A}F(\bar{G}) = \bar{A} \times F(\bar{G})$ , we see that for  $\bar{T} = \bar{A}F(\bar{G})$  that



$$|\bar{G} : \bar{G}'| \leq |\bar{T} : \bar{T}'|$$

Now let  $Z \leq T \leq G$  and  $Z \leq A \leq G$  be the inverse images of  $\bar{T}$  and  $\bar{A}$ , respectively.

Then  $T = AF(G)$  is a central product of  $A$  and  $F(G)$  with common central subgroup  $Z$ ; write  $T = A \wr_Z F(G)$ .

Let  $Z_1 = A' \leq Z$ ,  $Z_2 = F(G)' \cap Z$ , and  $Z_0 = Z_1 \cap Z_2$ . Then

$$T' = Z_1 \wr_{Z_0} F(G)'$$

and thus

$$|T : T'| = \frac{\frac{|A|}{|Z|} \frac{|F(G)|}{|Z|}}{\frac{|Z_1|}{|Z_0|} \frac{|F(G)'|}{|Z_0|}} = |A/Z| |F(G) : F(G)'| \frac{1}{|Z_1 : Z_0|}$$

Now observe that  $Z_1 \leq Z \cap G'$  and (by definition)  $Z_2 = Z \cap F(G)'$ . Thus  $Z_1 Z_2 \leq Z \cap G'$ , and so

$$Z_1/Z_0 = Z_1/(Z_1 \cap Z_2) \cong Z_1 Z_2/Z_2 \leq (Z \cap G')/(Z \cap F(G)')$$

Therefore

$$|T : T'| \geq |A/Z| |F(G) : F(G)'| \frac{|Z \cap F(G)'|}{|Z \cap G'|} \quad (2)$$

Now from (1) we get

$$\begin{aligned} |G : G'Z| &= |(G/Z) : (G/Z)'| = |\bar{G} : \bar{G}'| \\ &\leq |\bar{A}| |F(\bar{G}) : F(\bar{G})'| \\ &= |A/Z| |(F(G)/Z) : (F(G)/Z)'| \\ &= |A/Z| |F(G) : F(G)'Z| \\ &= |A/Z| \frac{|F(G)| |Z \cap F(G)'|}{|F(G)'| |Z|} \\ &= |A/Z| |F(G) : F(G)'| \frac{|Z \cap F(G)'|}{|Z|} \end{aligned} \quad (3)$$

so finally altogether we obtain with (3) and (2) that

$$\begin{aligned} |G : G'| &= |G : G'Z| |G'Z : Z| \\ &= |G : G'Z| |Z : (Z \cap G')| \\ &\leq |A/Z| |F(G) : F(G)'| \frac{|Z \cap F(G)'|}{|Z|} \frac{|Z|}{|Z \cap G'|} \\ &\leq |T : T'| \end{aligned}$$

and  $p$  does not divide  $|T|$ .

$T$  is a solvable group that acts faithfully on  $V$  and  $(|T|, p) = 1$ . It is clear that  $T$  acts completely reducibly on  $V$ . Thus  $|G : G'| \leq |T : T'| \leq$  the largest orbit of  $T$  on  $V \leq M$  by [5, Theorem 1.1]. □

### Acknowledgements

The first author was also partially supported by a grant from the Simons Foundation (#280770 to Thomas M. Keller). The second author would like to thank for the financial support from the AMS-Simons travel grant.

### REFERENCES

- [1] M. Aschbacher, R. M. Guralnick, ‘On abelian quotients of primitive groups’, Proc. Amer. Math. Soc. **107** (1989), 89–95.
- [2] W. Feit, ‘On large Zsigmondy primes’, Proc. Amer. Math. Soc. **102** (1988), 29–36.
- [3] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.
- [4] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the Finite Simple Groups, Number 2, AMS, Providence, RI, 1996.
- [5] T. M. Keller, Y. Yang, ‘Abelian quotients and orbit sizes of solvable linear groups’, Israel J. Math., accepted.
- [6] R.A. Wilson, The finite simple groups, Graduate Texts in Mathematics 251, Springer-Verlag London, Ltd., London, 2009.

DEPARTMENT OF MATHEMATICS, TEXAS STATE UNIVERSITY, 601 UNIVERSITY DRIVE, SAN MARCOS, TX 78666, USA.

*E-mail address:* `keller@txstate.edu`, `yang@txstate.edu`